

ANNEXE RGPD : NOTICE D'UTILISATION

ATTENTION : Les deux pages suivantes (notice d'utilisation) sont à usage pédagogique et strictement internes à la CDC ; elles doivent être supprimées avant tout envoi de l'Annexe RGPD aux prestataires ou toute publication en tant que pièce d'un marché.

Préalable : notions-clé.

Aux termes des présentes et du RGPD¹, sont entendus comme :

- « responsable de traitement » (RT) : la personne physique ou morale, l'autorité publique ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ;
- « sous-traitant » (ST) : la personne physique ou morale ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement.

Cas d'usage du document.

Cette Annexe « Sous-traitance de traitement de données à caractère personnel » (l'« Annexe RGPD ») a vocation à être intégrée à :

- ✓ **tout contrat de prestations de services ou marché** (ex. : CCAP, Contrat SaaS) impliquant le traitement de données personnelles, et
- ✓ **dans le cadre duquel la CDC est « responsable de traitement » et le(s) prestataire(s) « sous-traitant(s) »**, au sens de la réglementation applicable aux données personnelles.

Cas où cette Annexe RGPD n'a pas à être utilisée :

- ✗ **Lorsque le prestataire qui contracte avec la CDC est qualifié de « responsable de traitement »** au sens du règlement général de protection des données (RGPD)² : il n'y a alors pas de « sous-traitance de données », ce document n'a pas à être annexé au contrat de référence (marché, convention, etc.) ;
[Cas particulier : si le cocontractant est responsable de traitement mais que la CDC agit comme sous-traitant : dans ce cas, l'Annexe RGPD peut être utilisée, mais le contenu de l'annexe I doit être adapté en ce sens et l'annexe V supprimée].
- ✗ **Lorsque la prestation implique un transfert de données personnelles hors de l'Union Européenne (UE)³** (ex : le prestataire est situé hors de l'UE, le prestataire héberge les données sur des serveurs cloud hors de l'UE) : dans ce cas, les CCT « Transferts » de la Commission européenne – module 2 doivent être annexées au contrat en lieu et place de cette Annexe.
Cas particuliers : Si le pays hors de l'UE vers lesquels les transferts sont envisagés bénéficie d'une décision d'adéquation (cf. liste tenue à jour par la Commission Nationale de l'Informatique et des Libertés en France (Cnil)), vous pouvez signer cette Annexe RGPD comme si les données restaient sur le territoire de l'UE. Dans le cas de transferts vers les Etats-Unis, il faut en plus vérifier que le(s) prestataire(s) cocontractant(s) est/sont valablement certifié(s)⁴.

¹ Règlement (UE) 2016/679 du Parlement et du Conseil du 27 avril 2016, applicable aux traitements de données personnelles : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679>

² Pour la notion de « responsable de traitement » ou de « sous-traitant » et le choix des qualifications RGPD, se référer à la [Fiche pratique sur les qualifications et responsabilités des acteurs en matière de protection des données personnelles](#), ou saisir DAJCD-NDPI en cas de difficulté à déterminer ces qualifications.

³ Plus précisément, hors de l'Espace économique européen (EEE) : Union européenne, Norvège, Islande et Liechtenstein

⁴ En effet, depuis une [décision d'adéquation](#) en date du 10 juillet 2023, la Commission européenne a autorisé les transferts de données vers les Etats-Unis, **sous réserve toutefois que les sous-traitants / prestataires soient certifiés** valablement au titre du « Data Privacy Framework » (DPF), programme de certification américain tenu à jour par les autorités publiques américaines. Vous pouvez retrouver la liste des organismes certifiés au titre du DPF et le périmètre de leur certification à l'adresse : <https://www.dataprivacyframework.gov/list>. Il est important de vérifier les éléments suivants pour vous assurer de la validité dans

Lorsque la prestation implique un transfert de données personnelles hors de l'UE parce que **le sous-traitant à qui les données sont confiées effectue lui-même des transferts** de données vers des entités ou services hors de l'UE (ex. recours à des sous-traitants ultérieurs situés hors UE, recours à des prestataires *cloud* dont les serveurs sont hors UE) : dans ce cas, il appartiendra au prestataire, au regard des garanties qu'il s'engage à respecter en signant l'Annexe RGPD, de mettre en place de son côté des garanties appropriées afin d'encadrer valablement les transferts vers ses sous-traitants ultérieurs, conformément aux dispositions du RGPD et à la doctrine des autorités⁵.

Contenu de l'Annexe RGPD et marges de négociation.

L'Annexe RGPD reprend les [clauses contractuelles types \(CCT\) de la Commission européenne](#) préconisées pour encadrer les traitements de données personnelles dans le cadre d'une sous-traitance de données, afin de respecter les exigences posées par l'article 28 du RGPD (dont les dispositions sont impératives).

En application de la réglementation, le corps des CCT n'a pas vocation à être modifié, limitant ainsi les marges de négociation dont pourraient se prévaloir vos cocontractants quant au contenu de cette Annexe RGPD.

Le maintien des CCT au sein de l'Annexe RGPD est un gage de conformité au RGPD pour vos cocontractants et la CDC. C'est l'argument à leur présenter en cas de besoin (refus de recourir à cette annexe, demandes de modification).

Plus précisément, l'argument à leur faire valoir en cas de demande de leur part de modifier substantiellement l'Annexe RGPD est le principe d'« invariabilité » des clauses, stipulé à la Clause 2 de ces CCT incorporées ci-dessous. Le risque pour les parties serait la non-conformité des clauses de l'Annexe RGPD à l'article 28 du RGPD sur la sous-traitance de données, dont les dispositions sont impératives.

En revanche, pour vous guider dans la préparation de l'Annexe RGPD en lien avec les prestataires / cocontractants afin de l'adapter aux traitements de données propres au contrat :

- Les éléments en **jaune** au sein de l'Annexe RGPD doivent être complétés, et peuvent donc être négociés ;
- Les éléments en **bleu** sont des options contractuelles alternatives, qui impliquent de faire un choix ;
- Des précisions d'ordre opérationnel (ex. : sur la mise en œuvre pratique des traitements) ou des stipulations complémentaires (« garanties supplémentaires ») peuvent être ajoutées **en annexe V**, à condition qu'elles ne viennent pas contredire les CCT (ex. : annuler, rendre inopérantes, priver d'effet, limiter, conditionner... les dispositions prévues dans les CCT).

Complétion des annexes.

Les annexes de l'Annexe RGPD sont ainsi modifiables et négociables, puisque leur contenu doit impérativement être complété avant la signature, au regard des caractéristiques de la prestation objet du contrat et des traitements de données opérés pour les besoins de celle-ci.

Les annexes I à IV doivent être complétées sur la base de la fiche DCP en lien avec votre RDCP et/ou DPO, du questionnaire SaaS rempli par le prestataire et du Plan d'assurance sécurité⁶.

Pour toute question relative à l'utilisation de ce document, vous pouvez prendre contact avec l'équipe DAJCD/NDPI, Sylvain Rougeaux, responsable du département, ou Jean-Christophe Géret, responsable adjoint du département.

votre cas de figure de la certification de vos prestataires/sous-traitants, même s'ils figurent bien dans la liste des organismes certifiés : **date d'expiration de la certification, type des données et finalités de traitement couvertes par la certification (et enfin, pour les groupes d'entreprises, si besoin, entité(s) bénéficiaire(s) de la certification)**.

⁵ L'Annexe RGPD prévoit des garanties à cet égard ; pour plus d'explications sur la notion de « garanties appropriées » au sens de la réglementation ou sur les transferts de données hors EEE, se référer à la [Fiche juridique sur les transferts de données](#).

⁶ Pour en savoir plus sur la fiche DCP, veuillez-vous référer à la [Fiche service Next La protection dès la conception et ses supports](#) ; pour les deux autres documents, voir avec votre RSSI et/ou votre référent SaaS.

Appendix "Subcontracting of Personal Data Processing"

This Appendix ("**GDPR Appendix**") sets out the European Commission's standard contractual clauses under Article 28(7) of Regulation (EU) 2016/679, as derived from the Implementing Decision of 4 June 2021 (hereinafter, "**Article 28 SCCs**") aimed at providing a framework for the relationship between data controller and data processor within the meaning of the applicable regulations⁷.

The text of Article 28 SCCs incorporated below is unchanged.

Appendices I to IV are supplemented only insofar as they relate to the specific characteristics of personal data processing carried out in the context of the service covered by the contract.

An Appendix V containing additional *stipulations* to the Article 28 SCCs is added to the GDPR Appendix, in compliance with Clause 2 b) of the Article 28 SCCs below. The sole purpose of these stipulations is to complement the Article 28 SCCs in order to ensure their operational implementation and provide additional guarantees for the protection of individuals with regard to the processing of personal data. Under no circumstances may these stipulations have the effect of altering the content and nature of the Parties' commitments contained in the Article 28 SCCs, in compliance with applicable regulations.

In particular, Appendix V contains additional stipulations specific to international transfers (where applicable) to countries whose level of protection is not deemed adequate by the European Commission, and to the United States, in order to ensure that data transfers comply with the latest developments in applicable regulations.

In order not to modify the text of the Article 28 SCCs below, the term "contract" used below refers to the "Contract", "Procurement" or any other contractually defined term to designate the legal act under the terms and in the context of which the data processor processes data on behalf of the data controller, and to which the GDPR appendix is appended.

Where there is more than one data controller or processor designated in Appendix I, the terms "controller" and "processor" used in the singular, will refer respectively to each controller and processor referred to in Appendix I to the GDPR Appendix.

⁷The Commission's Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between data controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and Council, available at: <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32021D0915#d1e32-21-1>

**STANDARD CONTRACTUAL CLAUSES BETWEEN CONTROLLER AND PROCESSOR PURSUANT TO ARTICLE 28(7)
OF REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND COUNCIL**

THE EUROPEAN COMMISSION'S IMPLEMENTING DECISION (EU) 2021/915 OF 4 JUNE 2021

Contents

Standard contractual clauses	5
APPENDIX I - List of Parties	11
APPENDIX II – Description of processing	12
APPENDIX III - Technical and organisational measures, including those designed to ensure data security	12
APPENDIX IV - List of subsequent data processors	14
APPENDIX V - Additional stipulations	15
Article 1 – Hierarchy	15
Article 2 – Instructions	15
Article 3 – Documentation and compliance	15
Article 4 – Use of subsequent data processors	15
Article 5 – International transfers	16
Article 6 – Procedure in the event of an injunction from a third-country authority	17
Article 7 – Assistance to the data controller	18
Article 8 – Notification of personal data breaches	18
Article 9 – Noncompliance with clauses and termination	18

Standard contractual clauses

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with [choose relevant option: OPTION 1: Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)] / [OPTION 2: Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC].
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.
- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

- (a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- (b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- (c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1 Instructions

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- (b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

- (a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural

person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

OPTION 2: GENERAL WRITTEN AUTHORISATION : The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least [two months] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

- (b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- (d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

- (a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8
Assistance to the controller

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
- (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - (4) the obligations in [OPTION 1] Article 32 of Regulation (EU) 2016/679/ [OPTION 2] Articles 33 and 36 to 38 of Regulation (EU) 2018/1725.
- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9
Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:
 - (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (2) the likely consequences of the personal data breach;
 - (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679 /, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679 /.

SECTION III FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

APPENDIX I - List of Parties

Data controller(s):

The data controller is the Customer or Contracting Authority as designated in the Contract, and whose identity is stated below.

1. **Data controller's name and contact details:**

Caisse des Dépôts et Consignations
56, rue de Lille, 75007 Paris

2. Name, position and contact details of the contact person responsible for monitoring the Contract at the data controller's site (PDM):

[...]

Ms Wagner Virginie,
Direction des gestions d'actifs (GDA)
59, rue de Lille, 75007 Paris
Virginie.wagner@caissedesdepots.fr

3. Name and contact details of the data controller's DPO:

Ms Isabelle Guiomar,
Legal Affairs, Compliance and Ethics Department (DAJCD),
59, rue de Lille, 75007 Paris
dpo@caissedesdepots.fr

Data Processor(s):

The "data processor(s)" is/are the "Service Provider (s)" or "(joint) Holder(s)" of the Contract as defined herein, and whose identities are stated below.

1. Data processor's name and contact details:

[...]

2. Name, position and contact details of the contact person responsible for monitoring the Contract at the data processor's site :

[...]

3. Name and contact details of the data processor's DPO:

[...]

APPENDIX II – Description of processing

Name of the data processor to whom the processing of personal data has been subcontracted: [....]

Purpose of processing	Recording telephone conversations, SMS and MMS messages received and sent on asset managers' business cell phones as part of their asset management functions, in order to comply with legal obligations relating to market operations.
Purpose(s) for which personal data are processed on behalf of the data controller	GDA 02 - Manage listed and unlisted portfolios of CDC and its clients GDA 02 – Gérer les portefeuilles cotés et non cotés de la CDC et ses clients
Categories of personal data processed	Current personal data : surname, first name, function, business telephone number Communication : voice Logs : administrators' application logs (login details)
Categories of individuals concerned	Data controller's employees : asset managers, administrators External counterparts
Nature of processing operations	Collection, registration, storage, consultation
Duration of processing	Storage for 5 years : automatic purge after 5 years, or 7 years at the express request of the AMF. This storage period is determined by MAR regulation (art.16).
Transfer of data outside the EEA	<p>YES [] / NO []</p> <p><i>If yes, to which country/countries is/are the data transferred?</i> [complete]</p> <p><i>Is/are this/these country/countries included on the list held by the CNIL⁸, among the countries with adequate levels of protection (totally or partially)?</i> YES [] / NO []</p> <p><i>If the country in question only benefits from a partially adequate level of protection (e.g.: Canada and the United States), is the data processor considered to provide an adequate level of protection (e.g.: American data processor certified under the Data Privacy Framework (DPF) in the field covered by the processing)?</i> YES [] / NO []</p> <p><i>Are these data transfers carried out between the data controller and the data processor itself (tier 1 processor):</i> YES [] / NO []</p> <p>PLEASE NOTE: If transfers outside the EEA are made between the data controller and the processor itself (tier 1 processor), to countries considered non-adequate by the European Commission, <u>this GDPR Appendix cannot be used.</u></p> <p>The European Commission's "Transfers SCCs"⁹ - Module 2, <u>should then be used</u> to govern relations with the data processor, without prejudice to any additional measures that may be necessary depending on the level of protection afforded by the third country's law.</p>

APPENDIX III - Technical and organisational measures, including those designed to ensure data security

⁸ See the "Data protection in the world" map: <https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde>

⁹ The "Transfers SCCs" referred to as such herein are the European Commission's standard contractual clauses resulting from Commission Implementing Decision (EU) 2021/914 of 4 June 2021 bearing on standard contractual clauses for the transfer of personal data to third countries under Regulation (EU) 2016/679 of the European Parliament and Council (Text relevant to the EEA), accessible at the following address: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=fr
The "Transfers SCCs - Module 2" referred to as such herein are the European Commission's standard contractual clauses referred to above, adapted to govern transfers from controller to processor.

EXPLANATORY NOTE: Technical and organisational measures must be described in concrete, not generic terms. Where sensitive data is processed, as referred to in Clause 7.5 of the Article 28 SCCs, enhanced measures must be implemented, as described below. In the case of transfers of personal data to subsequent data processors, also describe the specific technical and organisational measures that the subsequent processor must take so as to be able to assist the data controller.

[Description of the technical and organisational security measures implemented by the data processor(s) (including any relevant certification) in order to ensure a level of security appropriate to the nature, scope, context and purpose of the processing, and the risks to the rights and freedoms of natural persons.

Examples of possible measures:

- *pseudonymisation and encryption of personal data;*
- *measures designed to ensure the processing systems' and services' ongoing confidentiality, integrity, availability and resilience;*
- *measures ensuring that means are in place to restore availability of and access to personal data within an appropriate timeframe in the event of a physical or technical incident;*
- *procedures for regularly testing, analysing and assessing the effectiveness of technical and organisational measures to ensure security of processing;*
- *user identification and authorisation measures;*
- *data protection measures during transmission;*
- *data protection measures during storage;*
- *measures designed to ensure the physical security of sites where personal data are processed;*
- *measures designed to ensure that events are recorded;*
- *measures designed to ensure system configuration, including default configuration;*
- *measures on governance and management of internal IT and IT security;*
- *certification/assurance measures for processes and products;*
- *measures designed to ensure data minimisation;*
- *measures designed to ensure data quality;*
- *measures designed to ensure limited data retention;*
- *measures designed to ensure accountability;*
- *measures enabling data portability and guaranteeing deletion].*

APPENDIX IV - List of subsequent data processors

OPTION 2

In the event of general authorisation of subsequent data processors, retained in Clause 7.7 of the Article 28 SCCs, the list of the data processor's subsequent processors is accessible:

- via the following URL link: [insert].
- in the absence of an online list: [specify the procedure for accessing the latest version].

The data processor undertakes to keep the list of subsequent data processor up to date.

APPENDIX V - Additional stipulations

Article 1 – Hierarchy

In addition to the provisions of Clause 4 of the Article 28 SCCs (as reproduced above), the Parties expressly acknowledge and agree that:

- 1.1. In the event of contradiction between the provisions of Appendices I to V and the provisions of the corpus of Article 28 SCCs, the provisions of the corpus of Article 28 SCCs shall prevail.
- 1.2. In the event of contradiction between any of the data processor's documents not appended *in extenso* hereto, and the provisions of the GDPR Appendix (including appendices), the provisions of the GDPR Appendix shall prevail.

Article 2 – Instructions

Clause 7.1 of the Article 28 SCCs is complemented by the following provisions:

- 1.1. The contract, its appendices, and in particular Appendices II to V hereof relating to the processing of personal data, provide documented instructions to the data processor within the meaning of Article 7.1 of the Article 28 SCCs.
- 1.2. Additional instructions may be provided by the data controller at a later date for the purposes of performing the service. Such additional instructions will then be sent in writing to the data processor, which undertakes to comply with them.

Article 3 – Documentation and compliance

Clause 7.6 of the Article 28 SCCs is complemented by the following provisions:

- 3.1. The data processor shall keep appropriate records of the processing activities carried out on behalf of the data controller.
- 3.2. The data controller may carry out audits, including of authorised data processors, in order to ensure compliance herewith and in particular to verify:
 - places where personal data are processed and/or stored;
 - transfers of personal data to countries outside the EEA;
 - measures taken to ensure the security of personal data and combat data breaches.
- 3.3. The data processor shall cooperate fully with any audit conducted in application hereof (and shall ensure that any subsequent data processors also cooperate), and with the data controller and/or any third party appointed by the controller for this purpose, including by giving them access to the premises, IT environments (physical and logical alike, whether hardware, software or networks), documentation, data relating to the services, and any useful information reasonably necessary in order to carry out the audit.
- 3.4. If, as a result of the audit measures, it is found that the security measures implemented by the processor are not appropriate or sufficient with regard to the characteristics of the processing, or if such audits reveal noncompliances herewith and/or with regard to the state of the art in the field, the processor shall implement any necessary corrective action – within a timeframe to be agreed between the Parties depending on the seriousness of the breach observed – without prejudice to the data controller's right to seek compensation for the harm suffered.
- 3.5. The costs of the audit shall be borne by the data processor in the event of any breach hereof observed during the audit.

Article 4 – Use of subsequent data processors

Clause 7.7 of the Article 28 SCCs is complemented by the following provisions:

- 4.1. Where the data processor envisages (i) using a new subsequent processor, or (ii) extending the scope of personal data processing operations entrusted to a subsequent processor authorised by the data controller (pursuant to the specific or general authorisation clause retained herein), the processor undertakes to

notify the following information by email to the Controller's contact person, whose contact details are specified in Appendix I "List of Parties", in compliance with the notice period in Clause 7.7:

- the subsequent data processor's identity and contact details;
- The reference of the contract or procurement concerned;
- the data processing operations envisaged;
- the location of outsourced processing operations;
- the desired effective date of the subcontract;
- in the event of a transfer to a country outside the EEA whose level is not recognised as adequate by the European Commission, the transfer tool used and additional measures implemented under Article 46 of the GDPR.

- 4.2. If the data controller objects to a change of subsequent processor, the processor shall, if necessary, propose another subsequent processor to the controller within thirty (30) days.
- 4.3. In the event that it is impossible to propose another subsequent data processor, or in the event of a further refusal by the data controller, which would make it impossible for the processor to perform the services in compliance with the requirements set out herein, the data controller shall be entitled to terminate the contract, under the conditions provided for in Article 9.2 below.
- 4.4. The obligation to subject the subsequent data processor to the same data protection obligations as those imposed on the data processor under the Article 28 SCCs, provided for in Clause 7.7 b), includes the obligations in this Appendix V "Additional Stipulations".

Article 5 – International transfers

Clause 7.8 of the Article 28 SCCs is complemented by the following provisions:

- 5.1. Where it intends to use a subsequent data processor in the context of the contract and such subcontracting would involve a transfer of data to a country outside the EEA, the data processor undertakes:
 - a) to implement the European Commission's Transfers SCCs - Module 3¹⁰ with each subsequent data processor concerned, if data transfers between the data processor and subsequent data processor(s) are not covered: (i) by an adequacy decision within the meaning of Article 45 of the GDPR (see the list maintained by the CNIL¹¹), (ii) or for the specific case of the United States, if the subsequent processor(s) is/are not included in the list of organisations certified under the DPF for the processing and/or data concerned, (iii) by binding corporate rules (BCR) within the meaning of Article 47 of the GDPR in the case of intra-group transfers, or (iv) by any other valid transfer control tool within the meaning of Article 46 of the GDPR;
 - b) prior to any transfer, to analyse the law of the third country to which the data is transferred, in order to determine whether the use of Transfers SCCs - Module 3 (or any other valid transfer tool within the meaning of Articles 46 ff. of the GDPR) would be sufficient to ensure the compliance of data transfers with applicable regulations (in particular 02/2020 Recommendations issued by the European Data Protection Board (EDPB)¹²;
 - c) in the event that Transfers SCCs - Module 3 (or any other transfer tool used) do not prove sufficient to guarantee an adequate level of data protection in accordance with applicable regulations: to add to Transfers SCCs - Module 3 (or to the transfer tool used) any additional measures necessary in order to comply with the requirements of the applicable regulations (in particular the EDPB's 01/2020 recommendations¹³).

¹⁰ The "Transfers SCCs - Module 3" referred to as such herein are the European Commission's standard contractual clauses, adapted for Module 3 applicable to processor-to-processor transfers:

https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=fr

¹¹ See the "Data protection in the world" map: <https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde>

¹² 02/2020 Recommendations on European Essential Guarantees for monitoring measures: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_fr

¹³ 01/2020 Recommendations on measures complementing transfer instruments designed to ensure compliance with the EU's level of personal data protection: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_fr

- 5.2. In determining what additional measures, if any, are necessary, the processor shall take account of the nature, importance, context and scope of the processing of personal data, as well as the risks to data subjects associated with the data's use.
- 5.3. All of these data transfer safeguards must be stipulated in the contract between the processor and any subsequent processor(s) called upon to process personal data outside the EEA. Upon request from the controller, the processor undertakes to provide a copy of the legal document governing the transfer of data between the processor and its subsequent processor(s), as well as any additional technical, legal and/or organisational measures implemented in order to provide the "appropriate guarantees" necessary to the said transfer of data outside the EEA.
- 5.4. The processor undertakes to verify at regular intervals that the various measures implemented ensure a level of personal data protection equivalent to that guaranteed by EU law. In the event of subcontracting involving transfer of data to the United States, to a certified member of the *Data Privacy Framework* (DPF) program¹⁴, the data processor undertakes to check each year that such certification is maintained for the scope of the data processing subcontracted. If it finds that this level is not or is no longer met, the processor undertakes to inform the controller without delay and to immediately suspend the transfer of personal data, as well as the subcontracting of personal data processing to the subsequent processor concerned.
- 5.5. When the processor carries out personal data processing on the basis of the DPF, it undertakes to maintain this certification for the entire scope of the data processing subcontracted, for the entire duration of the contract.
- 5.6. In the event of invalidation of the European Commission's adequacy decision concerning the United States, the Parties agree that the Transfers SCCs - Module 2 shall fully replace these Article 28 SCCs pending renegotiation of the contract between the Parties. However, the provisions of Appendices I to V hereto shall remain applicable between the Parties insofar as they are compatible with the Transfers SCCs – Module 2.

Article 6 – Procedure in the event of an injunction from a third-country authority

Clause 7.4 of the Article 28 SCCs is complemented by the following provisions:

In the event that the data processor receives an injunction from an authority in a third country seeking to compel it to disclose personal data processed under the contract:

- a) The processor agrees to inform the controller and, if possible, the data subject without delay (with the controller's assistance if necessary). (i) if it receives a legally binding request from a public authority, including a judicial authority, under the law of a third country for the disclosure of personal data processed hereunder; such notification shall include information on the personal data requested, the requesting authority, the legal basis of the request and the response provided; and/or (ii) if it becomes aware of any access by public authorities to personal data processed hereunder under the law of a third country, such notification shall include all information available to the processor.
- b) If the third country's legislation prohibits the processor from informing the controller and/or the data subject pursuant to a) above, the processor agrees to make every effort to obtain a lifting of such prohibition, with a view to communicating as much information as possible to the controller and/or the data subject, as soon as possible. The processor agrees to keep a documentary record of the efforts it has made to this end in order to be able to provide proof thereof to the controller.
- c) Where permitted by the third country's legislation, the processor shall provide the controller, at regular intervals, with as much useful information as possible on requests received from the authorities (number of requests, type of data requested, requesting authorities, etc.).
- d) Paragraphs a) to c) of this article are without prejudice to the processor's obligation to inform the controller without delay if it is unable to comply with the commitments made under the GDPR Appendix.
- e) The processor agrees to check the legality of the data disclosure request, in particular whether it falls within the limits of the powers conferred on the requesting public authority, and undertakes to contest it if it concludes that there are reasonable grounds for considering that it is illegal under the third

¹⁴ Since an [adequacy decision](#) of 10 July 2023, the European Commission has authorised data transfers to the United States, subject to the data processors to which the data is transferred being validly certified under the "*Data Privacy Framework*" (DPF), a US certification program maintained by the US public authorities. You can find the list of certified organisations and the scope of their certification here: <https://www.dataprivacyframework.gov/list>. **A number of points need to be checked regarding certification of the organisations on this list: the certification's expiry date, the type of data and processing purposes covered by the certification and, for groups of companies, which entity is the beneficiary of the certification, in order to be sure that it covers the transfer.**

country's legislation. When contesting a data disclosure request, the processor shall request provisional measures to suspend the effects of the request until the competent judicial authority has ruled on its merits. It shall not disclose the personal data requested unless it is obliged to do so pursuant to the procedural law applicable to it.

- f) The processor agrees to keep a documentary record of its legal assessment as well as of any contestation of the disclosure request and, insofar as the third country's legislation permits, to make the relevant documents available to the controller.
- g) The processor agrees to provide the strict minimum of information permitted when responding to a disclosure request, based on a reasonable interpretation of the request.

Article 7 – Assistance to the data controller

Clause 8 of the Article 28 SCCs is complemented by the following provisions:

When data subjects make requests to the processor to exercise their rights, the processor must email such requests as soon as they are received to the controller's contact person, whose contact details are specified in Appendix I "List of Parties", and ensure that they are received by the controller so that the latter can respond to them in due time.

Article 8 – Notification of personal data breaches

Clause 9 of the Article 28 SCCs is complemented by the following provisions:

- 8.1. Any breach of personal data shall be notified by email to the controller's contact person, whose contact details are specified in Appendix I. The processor shall ensure that the notification is received by the controller within twenty-four (24) hours.
- 8.2. In the event of a personal data breach relating to data processed by the controller, the processor shall assist the controller in notifying any competent supervisory authority of the personal data breach within a maximum period of twenty-four (24) hours after the controller becomes aware of the breach.
- 8.3. In the event of a personal data breach relating to data processed by the processor, the latter shall inform the data controller within a maximum of twenty-four (24) hours of becoming aware of the breach.
- 8.4. The processor undertakes not to inform any third party, including data subjects and the supervisory authority, of any personal data breach without the controller's prior written consent.
- 8.5. The processor shall take appropriate measures, at its own expense, to mitigate and remedy the consequences of any security incident at the origin of the personal data breach, and shall make any changes deemed necessary to ensure that similar incidents do not recur.

Article 9 – Noncompliance with clauses and termination

Clause 10 of the Article 28 SCCs is complemented by the following provisions:

- 9.1. Termination as provided for in Clause 10 b) shall be implemented under the conditions for termination for default provided for in the contract.
- 9.2. Termination due to the data controller's refusal of or objection to the subsequent processor proposed by the processor, as referred to in Article 4.3 above, shall be subject to a notice period of three (3) weeks as from notification of such termination by registered letter with acknowledgement of receipt, the effective date of termination being specified in the letter with regard to the characteristics of the service.
- 9.3. In the event of termination for any reason whatsoever as provided for herein, such termination: (i) shall give rise to reimbursement of any fees or amounts paid up to the end of the contract, (ii) shall take place at no cost or penalty to the data controller, and the Parties shall initiate the reversibility procedure provided for in the contract, at no cost to the data controller.